

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04N 7/167, H04K 1/00, H04L 9/00	A1	(11) International Publication Number: WO 98/27732 (43) International Publication Date: 25 June 1998 (25.06.98)		
(21) International Application Number: PCT/US97/22991		(81) Designated States: CA, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).		
(22) International Filing Date: 16 December 1997 (16.12.97)				
(30) Priority Data: 08/767,535 16 December 1996 (16.12.96) US		Published <i>With international search report. Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.</i>		
(71) Applicant: SCIENTIFIC-ATLANTA, INC. [US/US]; One Technology Parkway South, Norcross, GA 30092 (US).				
(72) Inventors: AKINS, Glendon, L., III; Apartment 409, 3250 Sweetwater Road, Lawrenceville, GA 30244 (US). BAKER, Robert, O.; 1581 Chamblee Gap Road, Cumming, GA 30130 (US).				
(74) Agents: PEZDEK, John, V. et al.; Scientific-Atlanta, Inc., One Technology Parkway South, Norcross, GA 30092 (US).				
(54) Title: PREVENTING REPLAY ATTACKS ON DIGITAL INFORMATION DISTRIBUTED BY NETWORK SERVICE PROVIDERS				
<p>(57) Abstract</p> <p>A technique for preventing replay attacks on digital information distributed by network services providers. At the beginning of a subscription period for a service, a network service provider sends entitlement messages to the subscriber which provide the subscriber for the service with a session key (110) and authorization information (214). The authorization information specifies a service (213) and a period of time (205). When an encrypted instance of a service is distributed on the network, it is accompanied by a series of entitlement control messages. Each of the messages includes a value which can be used with the session key to obtain a control word for decrypting the encrypted instance and a time specifier. The subscriber equipment which decrypts the instance of the service does so only if the time specifier in the entitlement control message specifies a time within the time period specified by the authorization information.</p>				

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon	KR	Republic of Korea	PL	Poland		
CN	China	KZ	Kazakhstan	PT	Portugal		
CU	Cuba	LC	Saint Lucia	RO	Romania		
CZ	Czech Republic	LI	Liechtenstein	RU	Russian Federation		
DE	Germany	LK	Sri Lanka	SD	Sudan		
DK	Denmark	LR	Liberia	SE	Sweden		
EE	Estonia			SG	Singapore		

Preventing Replay Attacks on Digital Information Distributed by Network Service Providers

Cross References to Related Applications

5

Background of the Invention

1. Field of the Invention

The invention generally concerns protecting digital information that is provided to users of a network by network service providers and more specifically concerns protecting the information against the class of attacks termed *replay attacks*, that is, attacks which work by replaying decryption information that the user received while he was subscribed to a service to decrypt information from the service after he has dropped his subscription.

15 2. Description of the Prior Art: FIG. 1

Fig. 1 shows how network service providers currently protect information which they distribute as part of a service from being viewed by network users who have not paid for the service. A service provider 105 employs network 111 to provide instances of services to a device 113 which is in the possession of a service subscriber who has subscribed for a period 20 of time to one or more services provided by service provider 105. Device 113 may take many forms. For example, if service provider 105 is a CATV broadcaster and network 111 is a CATV network, device 113 may be a set-top box; if service provider 105 is providing the service over the Internet, the device 113 may be a personal computer. As used here, an *instance* of a service is a single one of the items provided by the service. For example, if the 25 subscriber has subscribed for a service that offers a series of baseball games, each of the games is a single instance of the service.

Service provider 105 ensures that only subscribers to a service are able to view instances of the service by using encryption techniques as shown in FIG. 1. The techniques

require two transactions: a first transaction 101 takes place at the beginning of each subscription period, typically at the beginning of each month; the second transaction 103 takes place each time an instance of a service is distributed over network 111. In transaction 101, service provider 105 reads a subscriber data base 107 to determine for each subscriber which services the subscriber is to receive in the coming subscription period. When service provider 105 has determined what services the subscriber is entitled to, service provider 105 makes at least two entitlement messages (EMMs) and sends them to the subscriber's device 113. There are two kinds of EMM: a decryption EMM (DEMM) 108 which contains a *session key* 110 that will be used later to decrypt instances of one or more services to which the subscriber is entitled, and an authorization EMM (AEMM) 109 which contains a specification of the services the subscriber is entitled to. The specification appears in FIG. 1 as AI 113. Each subscription period, the subscriber receives DEMMs 108 and AEMMs 109 as required for the services the subscriber has subscribed to. Service subscriber device 113 stores the session keys 110 and the authorization information 113 received in the EMMs in secure memory 114. The saved information from the EMMs appears in FIG. 1 as SEMI 115.

A transaction 103 occurs each time service provider 105 sends an instance of the service to subscribers. What service provider 105 sends is of course an encrypted instance 117 of the service. In association with encrypted service instance 117, service provider 105 sends a series of entitlement control messages (ECMs) 119. Each ECM 119 corresponds to a part of encrypted service instance 117. An ECM 119 contains two kinds of information: one kind identifies the service that encrypted service instance 117 is an instance of; the other, shown in Fig. 1 as decryption information (DI) 120, is information which, when combined with the session key 110 stored in SEMI 115, permits decryption of encrypted service instance 117 in service subscriber device 113. When service subscriber device 113 receives ECM 119, it provides it to secure processor 116, which takes ECM 119 and SEMI 115 and uses the information contained therein as inputs to entitlement check module 121. Entitlement check module 121 first determines whether service instance 117 is an instance of one of the services currently authorized in SEMI 115 for the user. If it is, entitlement check

module 121 employs decryption information 120 and session key 110 to obtain instance key (IK) 123. Instance key 123 is often termed a *control word* in the arts to which the invention pertains. IK 123 is then used in decrypter 125 to decrypt encrypted service instance 117. Decrypted service instance 127 is thereupon provided to the user. The use of a series of 5 ECMs 119 with a single service instance 117 ensures that instance key 123 will change repeatedly while the service instance 117 is being broadcast and thereby reduces the incentive to a subscriber to make a copy of instance key 123 and distribute it electronically to others who would like to watch service instance 117 but have not paid for it. For further details on the kinds of systems just described, see *Specification des systemes de la famille 10 MAC paquets*, Document Technique 3258, Bruxelles: Centre technique de l'UER/EBU, Oct. 1986.

As is the case with any encryption scheme, the encryption scheme of FIG. 1 may be subject to various attacks by users who want access to an instance of a service but do not want to pay the subscription price for it. One such attack is the replay attack outlined above. 15 There are two variants of the attack. In the first variant, the pirate orders all services for the first month. The result is a transaction 101 in which the pirate receives EMMs for month one authorizing the full set of services. The pirate saves the AEMM 109 for that month. The second month, the pirate orders just enough services to receive a DEMM 108 with a session 20 key 110 for the desired service. The pirate allows session keys 110 to be processed by his subscriber device 113, but instead of providing the new month's AEMM 109, he provides the saved AEMM 109. At this point SEMI 115 has the session key for the second month together with the authorization information for the first month, and the pirate can thus decrypt instances of sevices in the second month even though he has not paid for them for that month.

25

In the second variant, the pirate has the minimum subscription for the first month. He records instances of an encrypted digital service that he has not subscribed to together with the ECMs 119 belonging to the instances. He also saves the current month's DEMM 108. The next month the pirate orders a subscription that includes the service that provided the

copied instances. When the pirate receives the AEMM 109 for the next month, he provides it together with last month's DEMM 108 to subscriber device 113. Having done this, the pirate also provides one of the saved instances of the digital service together with its ECMs 119 to subscriber device 113. Since SEMI 115 in subscriber device 113 now has both a session key 110 for the digital service to which the saved instance belongs and an authorization for that service, subscriber device 113 is able to use the ECMs 119 to decrypt the saved instance. It is an object of the invention disclosed herein to provide apparatus and methods for preventing such replay attacks.

10 Summary of the Invention

The invention deals with replay attacks by adding time information to the AEMM and the ECM. The AEMM contains a period specifier which specifies a period of time for which the AEMM is valid in addition to the service authorization information. When the service subscriber device receives the AEMM, it stores the period specifier and the service authorization information. When the service provider sends an instance of a service to the service subscriber device, it also sends an ECM. In addition to first decryption information and an identifier for the service the instance belongs to, the ECM of the invention contains a time value. When the service subscriber device receives the ECM, it uses the identifier for the service from the AEMM and the service authorization information from the ECM to verify that the subscriber is entitled to receive instances of the service and the period of time specifier from the AEMM and the time value from the ECM to verify that the AEMM is valid for the instance of the service associated with the ECM. If both verifications succeed, the service subscriber device uses previously received decryption information, and the first decryption information from the ECM to produce an instance key. Then the service subscriber device uses the instance key to decrypt or descramble the instance of the service.

25 Other aspects of the invention include techniques for encrypting the AEMM and techniques for deriving the instance key from the first and second decryption information.

The foregoing objects and advantages of the invention will be apparent to those skilled in the arts to which the invention pertains upon perusal of the following *Detailed Description* and drawing, wherein:

5 **Brief Description of the Drawings**

FIG. 1 is a block diagram of prior-art techniques used to protect instances of services;

FIG. 2 is a diagram of a DEMM 108 and an AEMM 109 in a preferred embodiment;

FIG. 3 is a diagram of how EMMS are processed in a secure processor in a preferred embodiment;

10

FIG. 4 is a diagram of an ECM 119 in a preferred embodiment;

FIG. 5 is a diagram of how an ECM 119 is processed in a secure processor in a preferred embodiment; and

FIG. 6 is a diagram of a CATV system which employs the invention.

15

The reference numbers in the drawings have at least three digits. The two rightmost digits are reference numbers within a figure; the digits to the left of those digits are the number of the figure in which the item identified by the reference number first appears. For example, an item with reference number 203 first appears in FIG. 2.

20

Detailed Description

The following *Detailed Description* will first show the EMMS employed in a preferred embodiment of the invention, will then show how the information in the EMMS is processed in a secure processor in the preferred embodiment, will next show an ECM 119 which is employed in the preferred embodiment, and will thereupon show how the secure processor uses the information from the EMMS and ECM 119 to detect and prevent replay attacks on the encryption system. Finally, the *Detailed Description* will show how the invention may be deployed in a CATV system.

EMMs: FIG. 2

Fig. 2 shows the relevant portions of DEMM 108 and AEMM 109 in a preferred embodiment. DEMM 108 contains a session key 110 for one or more services selected by the subscriber for the subscription period that DEMM 108 corresponds to. In a preferred embodiment, a given session key may be used to decrypt instances of more than one service; in other embodiments, there may be a one-to-one correspondence between session keys and services.

DEMM 108 in a preferred embodiment is protected against tampering by a number of standard encryption techniques. One of these is the use of a *message digest* to ensure that the contents of DEMM 108 have not been tampered with. A message digest is a value which is significantly shorter than the message itself, but is related to the message such that if the message changes, the message digest changes. In a preferred embodiment, the message digest is secure hash value 215. Secure hash value 215 is made by means of a hash function from the current value of session key 210. As will be explained in more detail later, when DEMM 108 arrives in device 113, session key 210 is again hashed using the same hash function. If the hash value is different from the hash value in field 215, DEMM 108 has changed, either because of a transmission error or because someone has tampered with it. Session key 110 is further encrypted using a public key for device 113, while secure hash value 215 is encrypted with a private key 219 known only to the service provider. For details on the encryption techniques used to protect the contents of DEMM 108, see Bruce Schneier, *Applied Cryptography*, John Wiley and Sons, New York, 1994.

AEMM 109 contains authorization data 214, which is the data used by entitlement checking module 121 to determine what services a subscriber is currently authorized to receive. The parts of authorization data 214 which are relevant to the present discussion are validation period specification 205, first entitlement ID 211, and service bit map 213. Validation period specification 205 in a preferred embodiment specifies a period of time for which AEMM 109 is valid by means of two items of data: ValidFromDate 207, which is the

date AEMM 109 is valid from, and ValidToDate 209, which is the date AEMM 109 is valid to. In other embodiments, the validation period may be specified, for example, by only a beginning or end date, by a date and a value representing a period of time, or simply by a value representing a period of time. Additionally, the validation period specification may 5 specify a period in which the subscriber may not receive instances of the service.

FirstEntitlementID 211 and service bit map 213 together indicate what services the user of device 113 which receives AEMM 109 is entitled to. Service bit map 213 in a preferred embodiment is a 256-bit long data item in which bits(0..255) represent services provided by the service provider. The value of a given bit indicates whether the user of device 113 is entitled to the service represented by the bit. FirstEntitlementID 211 maps a set of integers which currently represent the set of services provided by the service provider to the bits in service bit map 213. For example, if the integers representing the set of services have the range 500-756, FirstEntitlementID 211 will have the value 500 and the service represented by an entitlement ID of 510 will map to bit(10) in service bit map 312. Like DEMM 108, AEMM 109 employs a secure hash value 215 as a digest and as in DEMM 108, authorization data 214 is encrypted with public key 217, while secure hash value 215 is encrypted with service provider private key 219.

20 Processing EMMs in User Device 113

FIG. 3 shows how EMMs are processed in user device 113. Processing is done in secure processor 116, which may be implemented using a secure microprocessor and/or a secure ASIC. *Secure* in this context means that any attempt to tamper with microprocessor 303 and/or the ASIC will result in the loss of any information stored in the device. Also 25 included in user device 113 is secure storage 305, which is tamper-resistant in the same fashion as microprocessor 303. Stored in secure storage 305 are the private key 307 which is used to decrypt messages encrypted with public key 217 and the public key 315 used to decrypt messages encrypted with private key 219.

When secure microprocessor 303 receives an EMM, it employs private key 307 to decrypt encrypted message 304 of EMM 109. In the case of a DEMM 108, message 304 is a session key 110 and in the case of an AEMM 109, it is authorization data 214. Message 304 is decrypted in decryption module 309 to produce decrypted message 306. Message 306 goes to hash module 311 which employs the same hash function to hash message 306 as was used in the service provider to hash message 306 in service provider 105. If message 306 is unchanged from what it was in service provider 105, the hash will produce the same hash value. In order to obtain the original hash value, which is stored in encrypted form at 308 in the EMM, secure microprocessor 303 uses public key 315 to decrypt encrypted secure hash value 308. The resulting secure hash value 218 is compared in module 217 with the hash value produced at module 311. If they are the same, decrypted message 306 is identical to what was sent from service provider 105. When that is the case, the contents of message 306 are stored in secure memory 305, as shown by gate module 319 and arrow 321.

15 **ECM 119: FIG. 4**

FIG. 4 shows details of ECM 119 in a preferred embodiment. ECM 119 includes decryption information 120 and authorization data 407. In the preferred embodiment, decryption information 120 is an integer which may be used with a session key 110 for the service to which ECM 119's service instance belongs to generate instance key 121 that will decrypt the portion of the service instance with which ECM 119 is associated. In other embodiments, decryption information 120 may be the encrypted instance key 121. In such embodiments, decryption of the encrypted instance key with session key 110 for the service will produce the instance key used to decrypt or descramble the service instance. The next field is current time 401, which contains a time stamp indicating the time at which the service instance with which ECM 119 is associated is to be distributed over network 111. Next is EntitlementID 403, which indicates which service the service instance belongs to. MAC field 405, finally, is a message digest produced by a hash function from DI 120, current time 401, and EntitlementID 403. As before, the purpose of MAC 405 is to ensure that ECM 119 arrives at user device 113 with contents identical to the ones it had when it was created in

service provider 105.

Processing of ECM 119 in User Device 113: Fig. 5

Fig. 5 shows how ECM 119 is processed in secure microprocessor 303 of user device 113. First, decryption information 120 is encrypted in module 501 with session key 110 for the service to which the service instance associated with ECM 119 belongs to produce instance key 123. Then authorization data 407 and decryption information 120 go to module 311, where they are hashed in module 311 with the same hash function used to produce MAC 405 in ECM 119. If nothing has changed in ECM 119, the result has the same value as MAC 405. If that is the case, gate function 319 permits instance key 319 to pass on to gate function 505. Gate function 505 is in turn controlled by authorization logic 507, which compares authorization data 407 with stored authorization data 214. If the service identified by entitlement ID 403 is one of the services specified for user device 113 in service bit map 213 stored in SEMI 115 and current time 401 is within the period of time specified by valid period specifier 205 of SEMI 115, authorization logic 507 causes gating function 505 to output instance key 121 to decrypter 125, where it is used to decrypt the service instance associated with ECM 119. In a preferred embodiment, the index of the bit for the service in bit array 213 is computed by subtracting FirstEntitlementID 211 in SEMI 115 from EntitlementId 403.

As shown by the foregoing, the addition of validation period specification 205 to AEMM 109 and current time 401 to ECM 119 permits secure microprocessor 303 to determine whether the service instance was subscribed to in the period of time with which AEMM 109 is associated and thereby effectively counters both variants of the replay attack.

Employing the Invention in CATV Services: FIG. 6

One area in which embodiments of the invention may be employed with particular advantage is in providing instances of services via a CATV system. FIG. 6 shows a CATV system 601 in which the invention is employed. The main components of CATV system 601 are control facility 602, head end 603, network 605, set-top box 607, and TV set 609.

Control facility 602 contains subscriber data base 107 and key generator 106 and provides DEMM 108, AEMM 109, and ECM 119 to head end 603. A given control facility 602 may serve one or more head ends 603. Head end 603 further receives service instances 117. Head end 603 sends EMMs and ECMS 119, as well as service instances 117, via network 605 to set-top box 607. Network 605 will generally employ coaxial cable or fiber cable to transmit information from head end 603 to set-top box 607, but may also employ ordinary telephone lines or microwave radio emanating from a transmission tower or a satellite. No matter how it is implemented, network 605 is a broadcast network in the sense that every set-top box connected to network 605 receives everything sent by head end 603 via network 605.

5 Depending on the network implementation, there may further be communication between set-top box 607 and head end 603 or between set-top boxes and the set-top boxes 617 may be implemented in personal computers or other computer systems. Both EMMs and ECMS 119 are sent as packets of digital data, while service instance 117 may be sent either in digital or analog form.

10

15

As indicated above, EMMs are intended for individual subscribers. Each set-top box 607 consequently contains a packet detecting module 607 that detects packets sent on network 605. In the case of EMMs, packet detecting module 607 accepts an EMM only if it is directed to the set-top box 607 containing packet detecting module 607. When packet detecting module 607 detects such an EMM, it provides its contents to secure microprocessor 303, where it is processed as described above. Similarly, when packet detecting module 607 detects an ECM 119 on a channel currently being received by set-top box 607, it provides it to secure processor 116, which processes it as described above. If secure processor 116 determines that ECM 119 specifies an instance of a service that the subscriber to whom set-top box 607 belongs is entitled to receive, the secure processor uses ECM 119 and the information from the EMMs that the secure processor has received to produce instance key 121, which is in turn used in decrypter 125 to decrypt service instance 117 to produce decrypted service instance 127, which is sent to television set 609 or any other device which can display the service instance. If service instance 117 is in digital form,

20

25

instance key 121 will be used directly to decrypt the digital data representing service 117; if service instance 117 is in analog form, it will be scrambled before it is output from head end 603 and instance key 121 will be used to control the behavior of the analog descrambler which will descramble service instance 117.

5

Conclusion

10 The foregoing *Detailed Description* has shown to those skilled in the art how a validation period specifier in an EMM and a time stamp in an ECM may be used to defeat attempts to obtain instances of services for free by replaying service authorization information that stems from a period of time which does not include the time at which the instance is sent. The inventor has further disclosed the best mode presently known to him of implementing the invention.

15 While the presently-known best mode is implemented in a CATV system, it will be immediately apparent to those skilled in the arts to which the invention pertains that the techniques described herein can be used in any system for distributing services across a network in which a subscriber signs up to receive instances of a given service over a specified period of time. The system in which the invention is used may distribute the services via any 20 sort of broadcast network, but also via networks such as the Internet in which there is bidirectional communication via the network between the subscriber and the source of the service.

25 The preferred embodiment is implemented in a set-top box used with a CATV system, but could equally be implemented in a PC, in the TV set, or in any apparatus which is connected to a network used by a service provider and which has sufficient computational capability to perform the calculations required for the invention. It will further be apparent to those skilled in the art that the invention can be embodied in data structures other than the EMMs or ECMS disclosed herein and that different techniques than those disclosed herein can

be used to encrypt the EMM or its equivalent and to generate an instance key from the information contained in the EMM and ECM.

For all of the foregoing reasons, the *Detailed Description* is to be regarded as being
5 in all respects exemplary and not restrictive, and the breadth of the invention disclosed herein
is to be determined not from the *Detailed Description*, but rather from the claims as
interpreted with the full breadth permitted by the patent laws.

What is claimed is:

1. A method of protecting a given encrypted instance of a service that a service provider provides via a network to a subscriber,
the method being practiced in apparatus by means of which the subscriber accesses instances of the service for limited periods of time and the method comprising the steps of:
 5. receiving a first message from the service provider, the first message including at least a period specifier which specifies a given period of time and an authorization for the service;
 7. receiving a second message from the service provider, the second message being associated with the given instance and including at least an identification of the service, a time specifier which specifies a time, and first decryption information for the given instance;
 10. receiving the given instance; and
 11. using the first decryption information and second decryption information accessible to the apparatus to decrypt the given instance only if the identification of the service from the second message indicates the same service as the authorization therefor from the first message and the time specified by the time specifier from the second message is within the period specified by the period specifier from the first message.
1. 2. The method set forth in claim 1 wherein:
 2. the period specifier specifies an expiration time; and
 3. the step of using the first and second decryption information is performed only if the time specified by the time specifier is no later than the expiration time.
1. 3. The method set forth in claim 1 wherein:
 2. the period specifier specifies an earliest valid time; and
 3. the step of using the first and second decryption information is performed only if the time specified by the time specifier is later than the earliest valid time.
1. 4. The method set forth in claim 1 wherein:
 2. the period specifier specifies the period by means of a first time and a second time; and

3 the step of using the first and second decryption information is performed only if the
4 time specified by the time specifier is in the period specified by the first time and the second
5 time.

1 5. The method set forth in any of claims 1 through 4 wherein:
2 any of the steps of receiving the first message or receiving the second message
3 receives the first message or the second message from the network.

1 6. The method set forth in any of claims 1 through 4 wherein:
2 the apparatus has an address for receiving messages;
3 the method includes the step of storing the period specifier and the authorization in
4 the apparatus; and
5 the apparatus performs the step of storing only if the first message is addressed to the
6 apparatus.

1 7. The method set forth in any of claims 1 through 4 wherein
2 the apparatus includes a secure memory,
3 the first message is encrypted, and
4 the method further comprises the step of:
5 decryption the first message and storing the first message in the secure memory.

1 8. The method set forth in claim 7 wherein:
2 the first message further includes a digest value which is a result of a function applied
3 at least to the values of the period specifier and the authorization;
4 the digest value is encrypted in the first message differently from the remainder of the
5 first message; and
6 the method further includes the steps of
7 decryption the digest value;
8 using the function to derive a new digest value from at least the decrypted period

- 9 specifier and authorization; and
10 storing the decrypted period specifier and authorization in the secure memory only if
11 the digest value and the new digest value are the same.
- 1 9. The method set forth in claim 8 wherein:
2 at least the period specifier and the authorization are encrypted using a public key
3 belonging to the apparatus and the digest value is encrypted using a private key belonging to
4 the service provider.
- 1 10. The method set forth in any of claims 1 through 4 wherein
2 the service provider provides a plurality of the services,
3 the authorization specifies a subset of the plurality of the services, and
4 the second decryption information includes a plurality of session keys for the plurality
5 of services; and
6 the step of using the first and second decryption information employs a given one of
7 the session keys corresponding to the service to which the instance belongs to decrypt the
8 given instance and does not decrypt the given instance unless the identification of the service
9 from the second message indicates one of the services specified in the authorization.
- 1 11. The method set forth in any of claims 1 through 4 wherein:
2 the second decryption information is an integer value;
3 the first decryption information is a session key; and
4 the step of using the first and second decryption information includes the steps of
5 using the integer value and the session key to generate an instance key for the given
6 instance and
7 using the instance key to decrypt the instance.
- 8 12. A method of protecting a given encrypted instance of a service that a service provider
9 provides via a network to a subscriber,

10 the method comprising the steps performed by the service provider of:
11 sending a first message to apparatus by means of which the subscriber accesses
12 instances of the service for limited periods of time, the first message including at least a
13 period specifier which specifies a given period of time and an authorization for the service;
14 sending a second message to the apparatus, the second message being associated with
15 the given instance and including at least an identification of the service, a time specifier which
16 specifies a time, and first decryption information for the given instance, and
17 sending the given instance via the network to the apparatus,
18 the apparatus using the first decryption information and second decryption information
19 accessible to the apparatus to decrypt the given instance only if the identification of the
20 service from the second message indicates the same service as the authorization therefor from
21 the first message and the time specified by the time specifier from the second message is
22 within the period specified by the period specifier from the first message.

1 13. The method set forth in claim 12 wherein:
2 the period specifier specifies an expiration time; and
3 the apparatus uses the first and second decryption information only if the time
4 specified by the time specifier is no later than the expiration time.

1 14. The method set forth in claim 12 wherein:
2 the period specifier specifies an earliest valid time; and
3 the apparatus uses the first and second decryption information only if the time
4 specified by the time specifier is later than the earliest valid time.

1 15. The method set forth in claim 12 wherein:
2 the period specifier specifies the period by means of a first time and a second time ;
3 and
4 the apparatus uses the first and second decryption information only if the time
5 specified by the time specifier is in the period specified by the first time and the second time.

1 **16.** The method set forth in any of claims 12 through 15 wherein:
2 any of the steps of sending the first message or sending the second message sends the
3 first message or the second message via the network.

1 **17.** The method set forth in any of claims 12 through 15 wherein:
2 the apparatus has an address for receiving messages; and
3 the step of sending the first message sends the first message to the address.

4 **18.** The method set forth in any of claims 12 through 15 wherein
5 the apparatus includes a secure memory and
6 the method further comprises the step of:
7 encrypting the first message,
8 the apparatus decrypting the first message and storing the first message in the secure memory.

1 **19.** The method set forth in claim 18 wherein the method further includes the steps of:
2 making a digest value which is a result of a function applied at least to the values of
3 the period specifier and the authorization;
4 encrypting the digest value differently from the period specifier and the authorization;
5 and
6 adding the encrypted digest value to the message,
7 the apparatus operating to decrypt the digest value, use the function to derive a new digest
8 value from at least the decrypted period specifier and authorization, and
9 store the decrypted period specifier and authorization in the secure memory only if the digest
10 value and the new digest value are the same.

1 **20.** The method set forth in claim 19 wherein the step of encrypting the first message
2 includes the steps of
3 encrypting at least the period specifier and the authorization using a public key

4 belonging to the apparatus and encrypting the digest value using a private key belonging to
5 the service provider.

1 21. The method set forth in any of claims 12 through 15 wherein
2 the service provider provides a plurality of the services,
3 the authorization specifies a subset of the plurality of the services, and
4 the second decryption information includes a plurality of session keys for the plurality
5 of services; and

6 the apparatus employs a given one of the session keys corresponding to the service
7 to which the instance belongs to decrypt the given instance and does not decrypt the given
8 instance unless the identification of the service from the second message indicates one of the
9 services specified in the authorization.

1 22. The method set forth in any of claims 12 through 15 wherein:
2 the first decryption information is an integer value;
3 the second decryption information is a session key; and
4 the apparatus uses the integer value and the session key to generate an instance key
5 for the given instance and uses the instance key to decrypt the instance.

1 23. An entitlement management message used in a system for providing encrypted
2 instances of services to subscribers via a network, the subscribers accessing the
3 instances by means of apparatus coupled to the network and each subscriber having
4 subscribed for access to instances of the service for a period of time,
5 the entitlement management message comprising:
6 a period specifier which specifies the period of time and
7 an authorization for the service;
8 the apparatus responding to the entitlement management message by storing the contents
9 thereof for later use in determining whether to decrypt an instance of the service.

- 1 **24.** The entitlement management message set forth in claim 23 wherein:
2 the period specifier specifies an expiration time.

- 1 **25.** The entitlement management message set forth in claim 23 wherein:
2 the period specifier specifies an earliest valid time.

- 1 **26.** The entitlement management message set forth in claim 23 wherein:
2 the period specifier specifies the period by means of a first time and a second time.

- 1 **27.** The entitlement management message of claim 23 wherein:
2 the contents of the entitlement management message are encrypted,
3 the apparatus further responding to the entitlement management message by decrypting the
4 contents thereof.

- 1 **28.** The entitlement management message of claim 27 further comprising:
2 a digest value which is a result of a function applied at least to the values of the period
3 specifier and the authorization, the digest value being encrypted differently from the
4 remainder of the first message.

- 1 **29.** The entitlement management message of claim 28 wherein:
2 at least the period specifier and the authorization are encrypted using a public key
3 belonging to the apparatus and the digest value is encrypted using a private key belonging to
4 the service provider.

- 1 **30.** The entitlement management message of claim 23 wherein:
2 the service provider provides a plurality of the services; and
3 the authorization specifies a subset of the plurality of the services.

4 **31.** An entitlement control message used in a system for providing encrypted instances of
5 services to subscribers via a network, the subscribers accessing the instances by means
6 of apparatus coupled to the network and each subscriber having subscribed for access
7 to instances of the service for a period of time,
8 the entitlement control message being associated with an instance and comprising:
9 an identification of the service;
10 a time specifier which specifies a time; and
11 first decryption information for the given instance,
12 the apparatus using previously-stored second decryption information and the first decryption
13 information to decrypt the given instance only if the identification of the service from the
14 entitlement control message indicates the same service as a previously-stored authorization
15 therefor and the time specified by the time specifier is within a period specified by a
16 previously-stored period specifier.

1 **32.** The entitlement control message set forth in claim 31 herein:
2 the first decryption information is an integer value,
3 the second decryption information being a session key and the apparatus employing the
4 integer value and the session key to generate an instance key and employing the instance key
5 to decrypt the instance.

1 **33.** Apparatus coupled to a network for accessing encrypted instances of a service which
2 a service provider provides to a subscriber via the network, the subscriber being permitted by
3 the service provider to access instances of the service for limited periods of time and
4 the apparatus comprising:
5 a receiver that receives messages and the instances from the service provider via the
6 network;
7 a processor coupled to the receiver that processes the messages; and
8 a decrypter coupled to the processor and the receiver that decrypts the instances,
9 the messages including

10 a first message including at least a period specifier which specifies a given period of
11 time and an authorization for the service and

12 a second message associated with the given instance and including at least an
13 identification of the service, a time specifier which specifies a time, and first decryption
14 information for the given instance and

15 the receiver receiving the first and second messages and providing them to the
16 processor,

17 the processor using the first decryption information and second decryption information
18 accessible to the apparatus to enable the decrypter to decrypt an instance received in the
19 receiver only if the processor determines that the identification of the service from the second
20 message indicates the same service as the authorization therefrom from the first message and
21 the time specified by the time specifier from the second message is within the period specified
22 by the period specifier from the first message.

1 **34.** The apparatus set forth in claim 33 wherein:

2 the period specifier specifies an expiration time; and

3 the processor uses the first and second decryption information to enable the decrypter
4 to decrypt the instance only if the processor determines that the time specified by the time
5 specifier is no later than the expiration time.

1 **35.** The apparatus set forth in claim 33 wherein:

2 the period specifier specifies an earliest valid time; and

3 the processor uses the first and second decryption information to enable the decrypter
4 to decrypt the instance only if the processor determines that the time specified by the time
5 specifier is at least as late as the earliest valid time..

1 **36.** The apparatus set forth in claim 33 wherein:

2 the period specifier specifies the period by means of a first time and a second time; and

3 the processor uses the first and second decryption information to enable the decrypter

4 to decrypt the instance only if the time specified by the time specifier is within the period
5 specified by the first time and the second time.

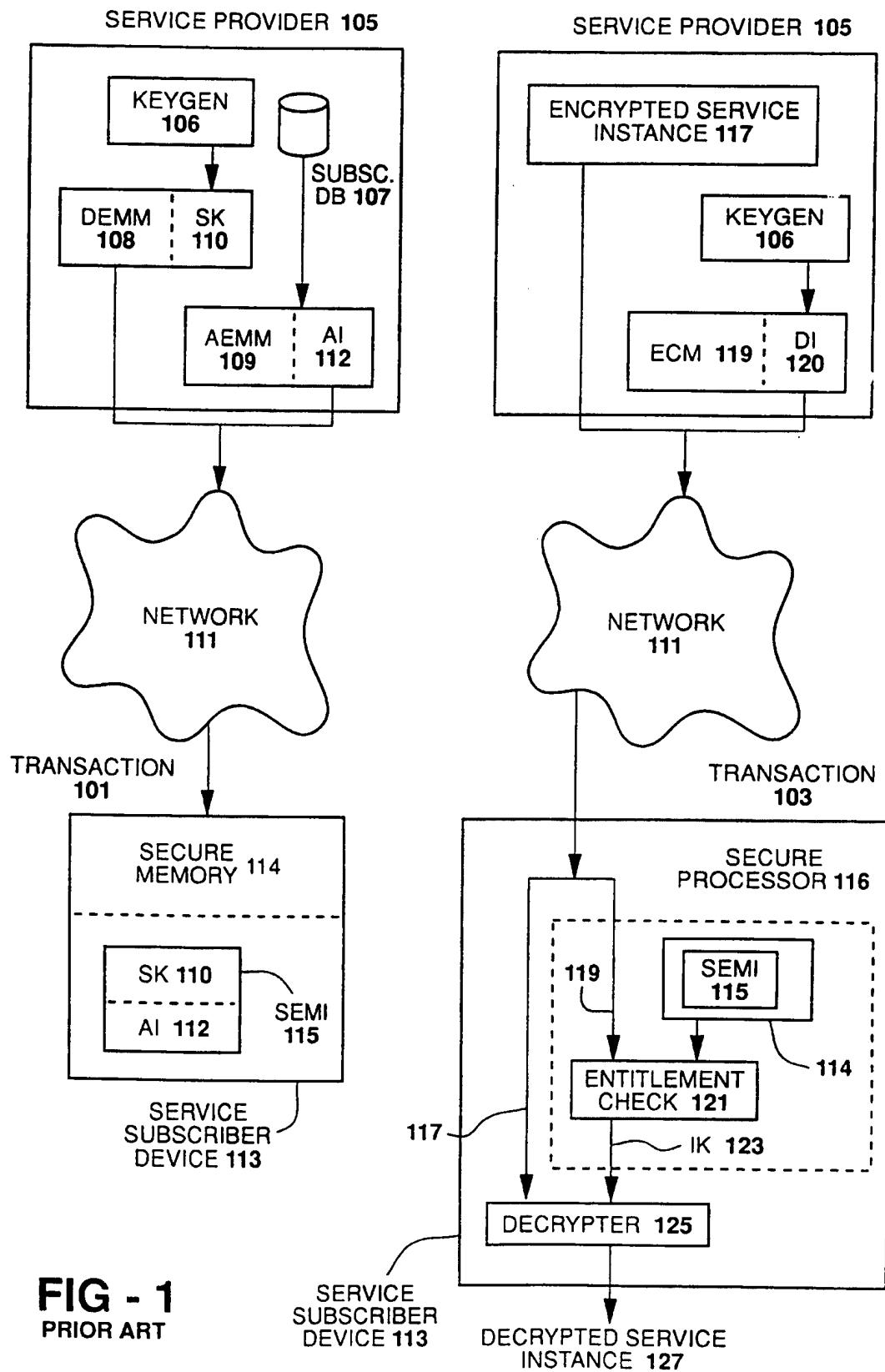
1 **37.** The apparatus set forth in any of claims 33 through 36 wherein:
2 the apparatus has an address for receiving messages;
3 the apparatus stores the period specifier and the authorization in the apparatus; and
4 the apparatus does the storing only if the first message is addressed to the apparatus.

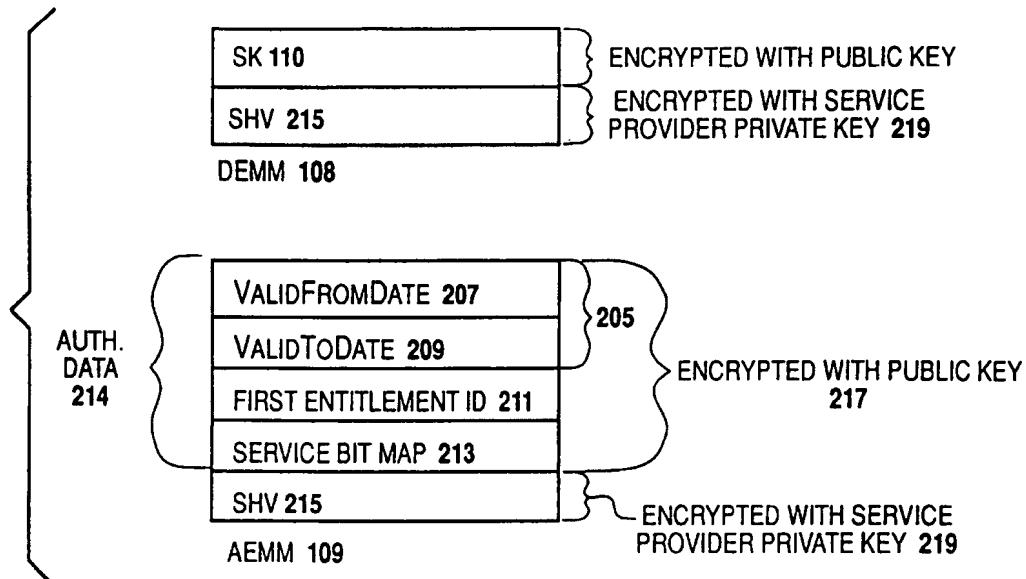
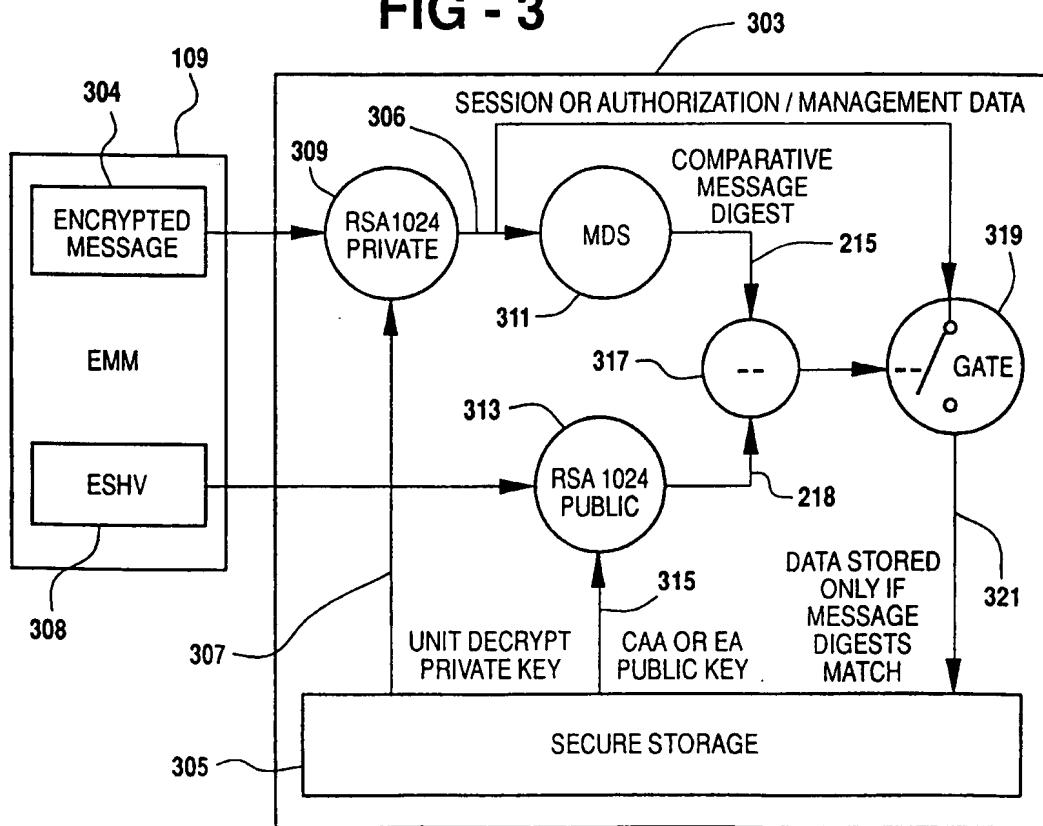
1 **38.** The apparatus set forth in any of claims 33 through 36 wherein
2 the apparatus includes a secure memory,
3 the first message is encrypted, and
4 the processor further decrypts the first message and stores the first message in the
5 secure memory.

1 **39.** The apparatus set forth in claim 38 wherein:
2 the first message further includes a digest value which is a result of a function applied
3 to the values of the period specifier and the authorization;
4 the digest value is encrypted in the first message differently from the remainder of the
5 first message; and
6 the processor further decrypts the digest value, uses the function to derive a new
7 digest value from at least the decrypted period specifier and authorization, and stores the
8 decrypted period specifier and authorization in the secure memory only if the digest value and
9 the new digest value are the same.

1 **40.** The apparatus set forth in claim 39 wherein:
2 the service provider encrypts at least the period specifier and the authorization using
3 a public key belonging to the apparatus and encrypts the digest value using a private key
4 belonging to the service provider.

- 1 **41.** The apparatus set forth in any of claims 33 through 36 wherein
2 the service provider provides a plurality of the services,
3 the authorization specifies a subset of the plurality of the services, and
4 the second decryption information includes a plurality of session keys for the plurality
5 of services; and
6 the processor employs a given one of the session keys corresponding to the service
7 to which the instance belongs to enable the decrypter to decrypt the given instance and does
8 not enable the decrypter unless the identification of the service from the second message
9 indicates one of the services specified in the authorization.
- 1 **42.** The apparatus set forth in any of claims 33 through 36 wherein:
2 the first decryption information is an integer value;
3 the second decryption information is a session key; and
4 the processor uses the integer value and the session key to generate an instance key
5 for the given instance and enables the decrypter by providing the instance key to the
6 decrypter.



**FIG - 2****FIG - 3**

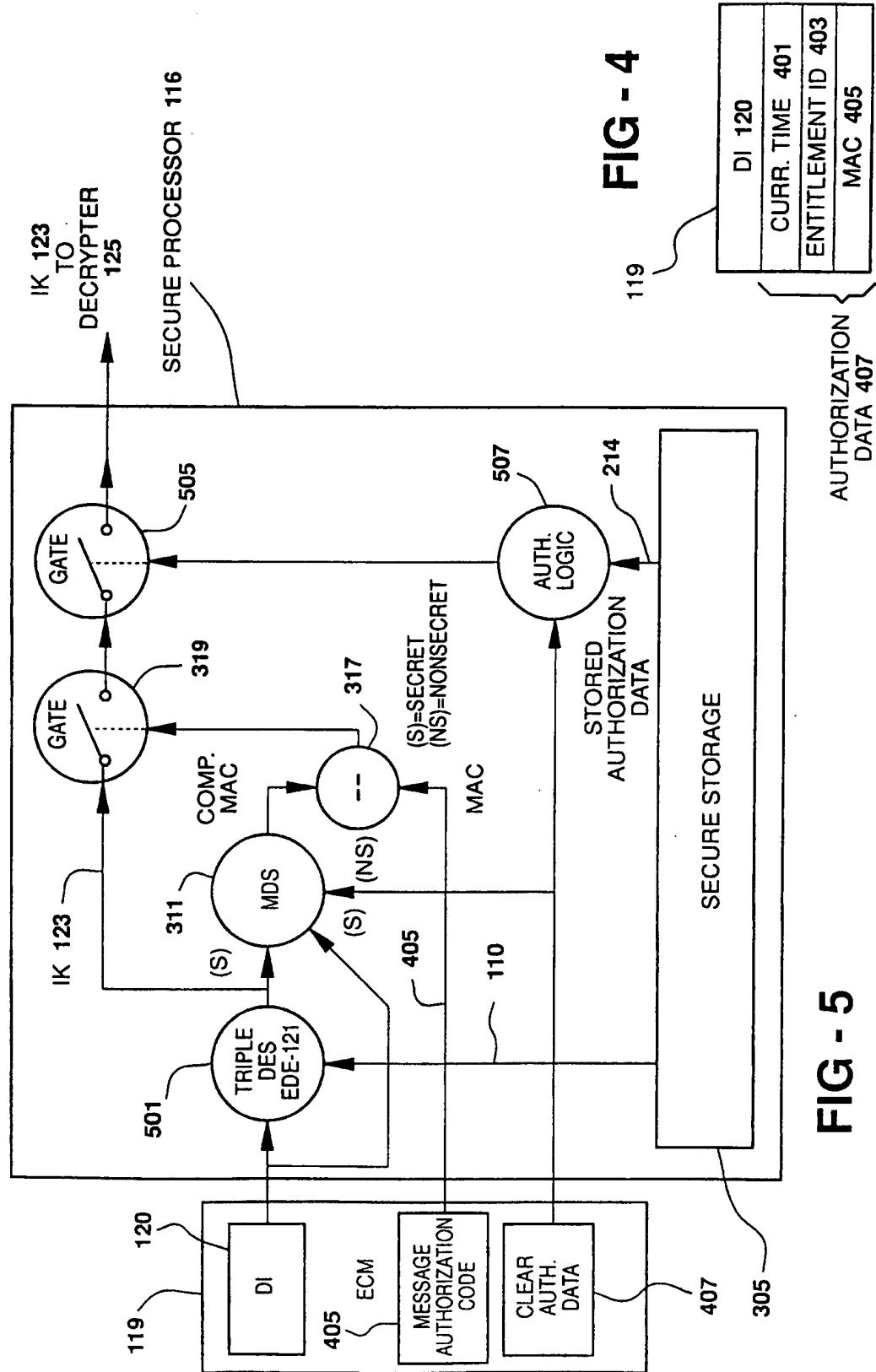
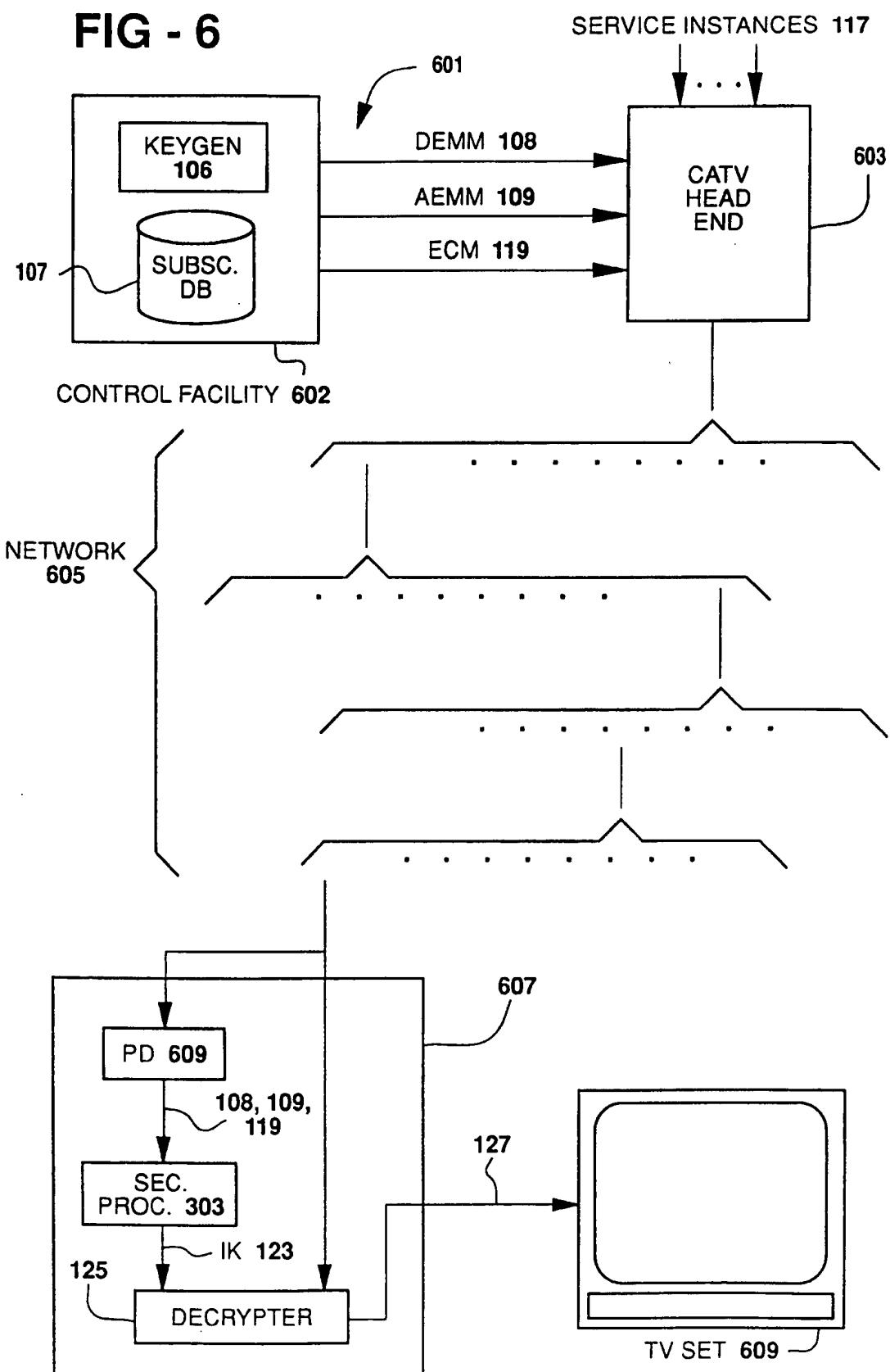


FIG - 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/22991

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :H04N 7/167; H04K 1/00; H04L 9/00
US CL :380/20, 21, 23, 49

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/20, 21, 23, 49, 30, 10, 48

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A, E	US 5,708,714 A (LOPEZ, et al.) 13 January 1998	1-42
A, E	US 5,724,424 A (GIFFORD) 03 March 1998	1-42
A, E	US 5,737,419 A (GANESAN) 07 April 1998	1-42
A	US 5,124,117 A (TATEBAYASHI, et al.) 23 June 1992	1-42
A	US 5,535,276 A (GANESAN) 09 July 1996	1-42
X	US 5,524,052 A (AUGUSTINE, et al.) 04 June 1996, see column 3 line 54 - column 6, line 55.	1-42

Further documents are listed in the continuation of Box C. See patent family annex.

* Special categories of cited documents:	*T*	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
A document defining the general state of the art which is not considered to be of particular relevance		
E earlier document published on or after the international filing date	*X*	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
L document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	*Y*	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
O document referring to an oral disclosure, use, exhibition or other means	*&*	document member of the same patent family
P document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search
13 APRIL 1998

Date of mailing of the international search report

14 MAY 1998

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703) 305-3230

Authorized officer
DAVID CAIN
Telephone No. (703) 305-1836